广西科学 Guangxi Sciences 2009,16(3):234～237

不相交差族(p^n,4,2)-DDF 的存在性*

The Existence of (p^n,4,2) Disjoint Difference Families

杨建效

YANG Jian-xiao

(陕西铁路工程职业技术学院,陕西渭南　714000)

(Shaanxi Railway Engineering Professional Technology Institute,Weinan,Shannxi,714000,China)

摘要:利用乘法特征和的 Weil 定理,结合计算机搜索来构造不相交差族,证明不相交差族 (p^n, 4,2)-DDF 的存在性,其中 $p \equiv 1 \pmod 6$ 为质数且 $n \geqslant 1$.

关键词:差族　不相交差族　特征和

中图法分类号:O157.2　**文献标识码**:A　**文章编号**:1005-9164(2009)03-0234-04

Abstract:By using Weil's theorem on character sum estimates, it is proved that there exists a (p^n, 4,2)-DDF, where $p \equiv 1 \pmod 6$ is a prime number and $n \geqslant 1$.

Key words:difference family,disjoint difference family,character sum

区组设计的研究是组合设计理论的核心内容.差族是区组设计的主要研究对象之一,它可以用来构造多种区组设计,很多学者对差族都进行过研究[1~4].本文利用乘法特征和的 Weil 定理,结合计算机搜索来构造不相交差族,证明 (p^n,4,2)-DDF 的存在性,其中 $p \equiv 1 \pmod 6$ 为质数且 $n \geqslant 1$.

1　预备知识

设 G 是一个 v 阶的 Abel 群,$\mathscr{B} = \{B_i | i \in I\}$,其中 B_i 是 G 的某些 k 元集合,$\Delta B_i = \{a - b | a,b \in B_i, a \neq b\}$,$\Delta\mathscr{B} = \bigcup \Delta B_i$.如果 $\Delta\mathscr{B}$ 使得 G 的每一个非零元恰好在其出现 λ 次,则称 $\mathscr{B}$ 是一个 (v,k,λ) 差族,记为 (v,k,λ)-DF,其中 B_i 称为基区组.如果一个 (v,k,λ)-DF 的基区组是不相交的,则称 (v,k,λ)-DF 是一个不相交差族,记为 (v,k,λ)-DDF.显然,(v,k,λ)-DDF 存在的必要条件为 $\lambda(v-1) \equiv 0 (\bmod k(k-1))$ 且 $\lambda \leqslant k-1$.设 $\mathscr{F} = \{F_0,F_2,\cdots,F_{s-1}\}$,其中每一个 F_i 都是一个 (v,k,λ)-DDF,如果 $\bigcup_{i=0}^{s-1} \bigcup_{B \in F_i} B$ 恰好是 $G - \{0\}$ 的一个划分,则称 $\mathscr{F}$ 是一个 (v,k,λ)-CDDF.从而,由 (v,k,λ)-CDDF 的存在性可知 (v,k,λ)-DDF 的存在性.

收稿日期:2009-03-05

作者简介:杨建效(1977-),男,硕士,主要从事组合数学研究。

* 国家自然科学基金项目(10561002)资助。

引理 1.1[2]　如果 $v \equiv 1 (\bmod 6)$,则存在 $(v,3,1)$-DDF.

引理 1.2[3]　设 $q - 1 = el$ 是一个奇质数幂,则存在 $(q,(q-1)/e,(q-1-e)/e)$-DDF.

当 $l = 3,4$ 时,有

引理 1.3　设 $q - 1 = 3e$ 是一个奇质数幂,则存在 $(q,3,2)$-DDF.

引理 1.4　设 $q - 1 = 4e$ 是一个奇质数幂,则存在 $(q,4,3)$-DDF.

引理 1.5[5]　设 $p \equiv 1 (\bmod 12)$ 是一个质数,$n \geqslant 1$,则存在 $(p^n,4,1)$-DDF.

引理 1.6[5]　如果在 $GF(q)$ 中存在 (q,k,λ)-DDF,则在 $GF(q^n)$ 中存在 (q^n,k,λ)-DDF.

2　主要结果

设 v 是一个质数幂,$F_v = GF(v)$,ζ 是 F_v 的本原元,$e | v - 1$,H 是 $F_v^* = F_v \backslash \{0\}$ 的 $(v-1)/e$ 阶乘法子群,$H^i = \zeta^i H$,$0 \leqslant i \leqslant e - 1$.

引理 2.1[3]　设 $e | v - 1$,B 是 F_v 的一个 k 元子集.如果 $\Delta B = \{a - b | a,b \in B, a \neq b\}$ 中的元素恰好在 H^0 的每一个陪集中分配 ω 个,则存在 (v,k,w)-DF;若 $2e | (v-1)$,则存在 $(v,k,w/2)$-DF.

设 $T_1 = \{a_i | i \in I\}$,$T_2 = \{b_j | j \in J\}$,记 $T_1 \circ T_2 = \{a_i b_j | i \in I, j \in J\}$.如果 $T_1 = \{a\}$,则 $T_1 \circ T_2 = aT_2 = \{ab_j | j \in J\}$.

引理 2.2　设 $v = 6t + 1$ 为质数幂,$H = \{1,\zeta^6,$

$\cdots,\zeta^{6(t-1)}\}$ 为 F_v^* 的 t 阶子群，$H^i=\zeta^i H, 0\leqslant i\leqslant 5$. 令 $M=\{1,x,x^2,x^3\}$，如果 $x, h_1(x), h_2(x)$ 满足下列条件之一：

(1) $x\in H^1, h_1(x)\in H^3, h_2(x)\in H^5$；

(2) $x\in H^1, h_1(x)\in H^4, h_2(x)\in H^3$；

(3) $x\in H^5, h_1(x)\in H^2, h_2(x)\in H^3$；

(4) $x\in H^5, h_1(x)\in H^3, h_2(x)\in H^1$，

则 $\mathscr{B}=\{M,\zeta^6 M,\cdots,\zeta^{6(t-1)}M\}$ 是一个 $(v,4,2)$-DDF，其中 $g_j(x)=x^j-1, h_{j-1}(x)=\dfrac{g_j(x)}{x-1}, 1\leqslant j\leqslant 3$.

证明 这里只证明满足条件(1)的情形，其它条件下的证明类似可以得到. M 中的各个元素之间的差为

1) $\pm\{g_1(x), xg_1(x), x^2g_1(x)\}=\pm(x-1)\{1,x,x^2\}$；

2) $\pm\{g_2(x), xg_2(x)\}=\pm(x-1)\{h_1(x), xh_1(x)\}$；

3) $\pm\{g_3(x)\}=\pm(x-1)\{h_2(x)\}$.

由于 M 中的元素位于不同的陪集 H^i 中，所以 $\mathscr{B}$ 中的元素是两两不相交的. 若 $x, h_1(x), h_2(x)$ 满足引理 2.2 中的条件(1)，则 $\Delta\mathscr{B}=2(GF(v)\backslash\{0\})$，故 $\mathscr{B}$ 是一个 $(v,4,2)$-DDF.

引理 2.3[6] 令 ψ 为 $GF(q)$ 的 m 阶乘法特征，$m>1$，$f(x)\in GF(q)[x]$ 为首 1 正次数多项式，且不是某多项式的 m 次幂，d 为 $f(x)$ 在扩域中相异根的个数，则对任意的 $\alpha\in GF(q)$，有

$$\left|\sum_{c\in GF(q)}\psi(\alpha f(c))\right|\leqslant(d-1)\sqrt{q}. \qquad (1)$$

引理 2.4 若 $v\equiv 1(\mathrm{mod}6)$ 为质数幂，且 $v\geqslant 256036$，则存在 $(v,4,2)$-DDF.

证明 利用引理 2.2 和 Weil 定理来构造 $(v,4,2)$-DDF. 令 $f_1(x)=\zeta^{-1}x, f_2(x)=\zeta^{-3}(x+1), f_3(x)=\zeta^{-5}(x^2+x+1)$，则引理 2.2 中的条件(1)可以转化为是否存在元素 $x\in F_v^*$ 满足：(i) $f_i(x)\in H^0$，$1\leqslant i\leqslant 3$.

在 $GF(v)$ 中，令 χ 为 6 阶的非平凡乘法特征，也就是说，当 $x\in H^j$ 时 $\chi(x)=\theta^j, 0\leqslant j\leqslant 5$，其中 $\theta=\exp(\dfrac{\pi i}{3})$ 为 6 次单位根. 令 $B_i=\chi(f_i(x))$ 且 $D_i=1+B_i+\cdots+B_i^5, 1\leqslant i\leqslant 3$. 则

$$D_i=\begin{cases}6, \text{if } f_i(x)\in H^0,\\ 1, \text{if } f_i(x)=0,\\ 0, \text{if } f_i(x)\notin H^0\cup\{0\}.\end{cases}$$

再令

$$S=\sum_{x\in GF(v)}\prod_{i=1}^{3}(1+B_i+\cdots+B_i^5). \qquad (2)$$

则 S 等于 $6^3 n+d$，其中 n 为 $GF(v)$ 中满足条件(i)的元素 x 的个数，d 为 $f_i(x)$ 为 0 时对和 S 的贡献，$1\leqslant i\leqslant 3$. 对任意的 $1\leqslant i\leqslant 3$，如果 $f_i(x)=0$，则对 S 的贡献最多为 6^2. 因此，如果 $|S|>6^3+3\times 6^2=324$，则在 F_v^* 中至少有一个元素 x 满足条件(i).

将 S 展开得

$$S=\sum_{x\in GF(v)}1+\sum_{i=1}^{3}\sum_{k=1}^{5}\sum_{x\in GF(v)}B_i^k+\sum_{1\leqslant i_1<i_2\leqslant 3}\ \sum_{1\leqslant k_1,k_2\leqslant 5}\ \sum_{x\in GF(v)}B_{i_1}^{k_1}B_{i_2}^{k_2}+\sum_{1\leqslant k_1,k_2,k_3\leqslant 5}\ \sum_{x\in GF(v)}B_1^{k_1}B_2^{k_2}B_3^{k_3}. \qquad (3)$$

使用有限域中乘法特征和的 Weil 定理来估计(2)式中 S 的最小值. 显然，$f_1(x), f_2(x), f_3(x)$ 两两互素. 设 $G(x)=f_1(x)^{\alpha_1}f_2(x)^{\alpha_2}f_3(x)^{\alpha_3}$ 为正次数多项式，可以证明，当 $\alpha_j\leqslant 5, 1\leqslant j\leqslant 3$ 时，$G(x)$ 不可能为 $GF(v)[x]$ 中的一个多项式的 6 次幂. 事实上，如果 $G(x)=p(x)^6$，由于 $f_1(x), f_2(x), f_3(x)$ 是两两互素的，所以 $\alpha_1\equiv\alpha_2\equiv\alpha_3\equiv 0(\mathrm{mod}6)$. 又因为 $\alpha_j\leqslant 5, 1\leqslant j\leqslant 3$，所以有 $\alpha_1=\alpha_2=\alpha_3=0$，与假设矛盾. 因为可以找到相应的 c 使得(2)式中的每一项乘积都表示成 $\psi(cf(x))$ 的形式，其中 $f(x)$ 是首一多项式. 易见，$\deg(f_1(x))=1, \deg(f_2(x))=1, \deg(f_3(x))=2$. 所以，由引理 2.3，有

$$\left|\sum_{i=1}^{3}\sum_{k=1}^{5}\sum_{x\in GF(v)}B_i^k\right|\leqslant 5(2-1)\sqrt{v}=5\sqrt{v},$$

$$\left|\sum_{1\leqslant i_1<i_2\leqslant 3}\ \sum_{1\leqslant k_1,k_2\leqslant 5}\ \sum_{x\in GF(v)}B_{i_1}^{k_1}B_{i_2}^{k_2}\right|\leqslant 5^2(1+1-1+2+1-1+2+1-1)\sqrt{v}=125\sqrt{v},$$

$$\left|\sum_{1\leqslant k_1,k_2,k_3\leqslant 5}\ \sum_{x\in GF(v)}B_1^{k_1}B_2^{k_2}B_3^{k_3}\right|\leqslant 5^3(2+1+1-1)\sqrt{v}=375\sqrt{v}.$$

从而 $|S|\geqslant v-(5+125+375)\sqrt{v}=v-505\times\sqrt{v}$. 如果 $v-505\sqrt{v}>324$，即 $v\geqslant 256036$，则 $n\geqslant 1$. 引理 2.4 证明完毕.

引理 2.5 设 $v\equiv 1(\mathrm{mod}6)$ 为质数且 $v\in[7,256036)$，$v\notin E$，则存在 $(v,4,2)$-DDF，其中 $E=\{7,13,19,31,37,43,61,73,79,103,109,127,139,181,223,241,307,313,331,367,379,439,463,487,499,619,787,859,1123\}$.

证明 通过计算机搜索，对于 $v\equiv 1(\mathrm{mod}6)$ 的质数且 $v\notin E$，满足引理 2.2 中的条件(1)的元素 $x\in F_v^*$ 全部找到. 表 1 列出当 $v\leqslant 600$ 时所有的数组 (v,ζ,x)，其中 ζ 为 F_v 的本原元. 而对其它的质数，由于篇幅关系，在这里不一一列出.

令 $E=A\cup B\cup C$，其中 $A=\{7,37,73,139,$

223,241,307,313,367,439,499,619,787,859,1123},$B=\{181,331,379,463,487\}$,$C=\{13,19,31,43,61,79,103,109,127\}$.

表1 数组(v,ζ,x),$v\leqslant 600$

Table 1 Array (v,ζ,x),$v\leqslant 600$

v	ζ	x	v	ζ	x	v	ζ	x
67	2	2	271	6	172	421	2	407
97	5	41	277	5	72	433	5	267
151	6	130	283	3	166	457	13	339
157	5	6	337	10	65	523	2	242
163	2	109	349	2	215	541	2	331
193	5	70	373	2	349	547	2	88
199	3	75	397	5	61	571	3	369
211	2	131	409	21	62	577	5	562
229	6	140						

引理 2.6 设$v\in A$,则存在$(v,4,2)$-DDF.

证明 通过计算机搜索,对于$v\equiv 1(\bmod 6)$的质数且$v\in A$,满足引理2.2中条件(2)的元素$x\in F_v^*$全部找到.表2列出所有的数组(v,ζ,x),其中ζ为F_v的本原元.

表2 数组(v,ζ,x)

Table 2 Array (v,ζ,x)

v	ζ	x	v	ζ	x	v	ζ	x
7	3	3	241	7	230	499	7	19
37	2	20	307	5	263	619	2	578
73	5	68	313	10	10	787	2	62
139	2	119	367	6	239	859	2	843
223	3	198	439	15	404	1123	2	315

引理2.7 设$v=6t+1$为质数幂,H为F_v^*中的$2t$阶子群,$H^i=\zeta^i H,0\leqslant i\leqslant 2$.令$T=\{1,\zeta^3,\cdots,\zeta^{3(t-1)}\}$,$M=\{1,x,x^2,-1\}$,如果还满足下列条件之一:

(1)$2\in H^1,x\in H^1,x-1\in H^0,x^2+1\in H^0,x+1\in H^2$;

(2)$2\in H^1,x\in H^1,x-1\in H^1,x^2+1\in H^0,x+1\in H^2$;

(3)$2\in H^1,x\in H^1,x-1\in H^2,x^2+1\in H^1,x+1\in H^0$;

(4)$2\in H^1,x\in H^1,x-1\in H^2,x^2+1\in H^2,x+1\in H^1$;

(5)$2\in H^1,x\in H^1,x-1\in H^2,x^2+1\in H^0,x+1\in H^2$;

(6)$2\in H^1,x\in H^2,x-1\in H^1,x^2+1\in H^2,x+1\in H^2$;

(7)$2\in H^1,x\in H^2,x-1\in H^2,x^2+1\in H^0,x+1\in H^0$,

则$\mathscr{B}=\{M,\zeta^3 M,\cdots,\zeta^{3(t-1)}M\}$是一个$(v,4,2)$-DDF.

证明 这里只证明满足条件(1)的情形,其它条件下的证明类似可得.M中的各元素之差为

1) $\pm\{x-1,(x+1)(x-1),2\}$;

2) $\pm\{x(x-1),x+1\}$;

3) $\pm\{x^2+1\}$.

由于$\zeta^{6t}=1$,所以$\zeta^{3t}=-1$,$-1\in H^0$,$T\cup\{-T\}=H$.显然,$\mathscr{B}$中的元素是两两不相交的.若引理2.7中的条件(1)成立,则$\Delta\mathscr{B}=2(GF(v)\backslash\{0\})$,故$\mathscr{B}$是一个$(v,4,2)$-DDF.

注 当$2\in H^0$或$2\in H^2$时,可以将$x,x-1,x^2+1,x+1$所在的陪集作适当的调整,在此仅以$2\in H^1$进行讨论.

引理 2.8 若$v\in B$,则存在$(v,4,2)$-DDF.

证明 通过计算机搜索,在表3中列出了相应的数组(v,ζ,x),其中ζ为F_v的本原元,$x\in F_v^*$中的元素满足引理2.7中的条件(1).

表3 数组(v,ζ,x)

Table 3 Array (v,ζ,x)

v	ζ	x	v	ζ	x	v	ζ	x
181	2	2	379	2	2	487	3	239
331	3	227	463	3	335			

引理2.9 若$v\in C$,则存在$(v,4,2)$-DDF.

证明 通过计算机的直接搜索,找到了相应的$(v,4,2)$-DDF,结果如下:

$v=13$,

$\mathscr{B}$:{0,1,3,9},{2,4,7,8};

$v=19$

$\mathscr{B}$:{0,1,2,8},{3,10,13,18},{5,9,11,14};

$v=31$,

$\mathscr{B}$:{1,15,17,21},{2,28,29,30},{3,13,19,27},{5,14,23,26},{4,11,16,24};

$v=43$,

$\mathscr{B}$:{0,20,30,28},{1,12,19,29},{2,7,41,42},{3,9,21,40},{5,6,10,32},{11,14,25,38},{13,27,34,36};

$v=61$,

$\mathscr{B}$:{0,7,26,44},{1,21,35,60},{2,33,37,42},{4,14,50,53},{6,17,20,54},{10,25,41,48},{11,16,24,56},{19,38,39,47},{22,28,32,34},{29,40,57,58};

$v=79$,

$\mathscr{B}$:{0,27,56,77},{3,37,51,78},{4,12,13,76},{5,22,44,65},{6,39,45,69},{8,33,38,52},{9,21,34,47},{14,50,61,67},{15,20,35,57},{23, 24,68,70},{30,40,48,58},{31,55,59,62},{43,54,63,66};

$v=103$,

$\mathscr{B}$: {0,18,31,80}, {3,29,51,81}, {4,42,57,89},{5,41,74,82},{26,33,38,78},{9,13,14,16},{10,20,76,96}, {12,34,36,69}, {19,55,61,85},{24,27,43,72},{25,54,63,79},{6,7,49,95},{32,60,71,92},{44,50,84,94},{48,59,67,87},{53,66,70,97},{56,68,77,91};

$v=109$,

$\mathscr{B}$: {0,7,50,81}, {4,56,76,96}, {5,26,37,83},{6,36,51,61},{9,21,69,80},{10,74,75,92},{13,43,62,85}, {14,24,65,90}, {15,27,29,63},{16,42,55,71}, {17,33,39,41}, {22,31,35,58},{25,34,72,101},{28,46,49,102},{40,64,79,105},{44,78,84,106}, {57,89,103,108}, {99,100,104,107};

$v=127$,

$\mathscr{B}$: {1,54,84,104},{2,61,68,90},{3,39,92,110}, {4,17,67,86}, {5,75,80,124}, {6,18,52,107},{10,37,43,91},{15,103,113,121},{16,95,106,109},{21,25,26,120},{23,33,48,108},{24,82,89,114},{27,46,62,93},{29,6978,105},{30,72,81,112},{31,53,94,96},{34,49,60,77},{40,64,70,87},{41,44,57,98},{50,51,118,122},{76,97,99,111}.

定理 2.1 设 $v\equiv 1(\mathrm{mod}6)$ 是一个质数,则存在 $(v,4,2)$-DDF.

证明 引理 2.4 给出当 $v\geqslant 256036$ 时,$(v,4,2)$-DDF 的存在性.引理 2.5,引理 2.6,引理 2.8 和引理 2.9 给出当 $v\in[13,256036)$ 时,$(v,4,2)$-DDF 的存在性,所以定理 2.1 成立.

由引理 1.6 和定理 2.1,有

定理 2.2 设 $p\equiv 1(\mathrm{mod}6)$ 是一个质数,$n\geqslant 1$,则存在 $(p^n,4,2)$-DDF.

参考文献:

[1] Chang Y,Ding C. Constructions of external difference families and disjoint difference families[J]. Des Codes Crypt,2006,40:167-185.

[2] Dinitz J H,Rodency P. Disjoint difference families with block size 3[J]. Util Math,1997,52:153-160.

[3] Wilson R M. Cyclotomy and difference families in elementary abelian groups[J]. J Number Theory,1972,4:17-47.

[4] Fuji-Hara R,Miao Y. Complete sets of disjoint difference families and their applications[J]. J Statistical Planning and Inference,2002,106:87-103.

[5] 杨建效. 不相交差族 $(p^n,4,1)$-DDF 的存在性[J]. 广西科学,2008,15(3):218-220.

[6] Lidl R,Niederreiter H. Finite fields,encyclopedia of mathematics and its applications [M]. Cambridge: Cambridge University Press,1983:20.

(责任编辑:尹 闯)

美国科学家首次发现调控人类睡眠的基因

就目前所知,睡眠在很大程度上由两种机制调控:一是昼夜节律,在24小时内,人体的生理生化机制会出现盛衰变化,从而调节睡眠时间;二是体内状态平衡机制,它确保人体在经过必要时间的睡眠后能够得到恢复,使人能够在身体需要时睡觉,在已经得到满足时醒来。昼夜节律和体内平衡机制的相互作用,影响着睡眠的时间点、长度、质量以及醒后人体的各种机能状况。

美国科学家在一个小型家庭的研究中发现,母亲和其成年女儿每日的睡眠需求一直都远比其他人少。科学家就母亲及其大家庭中其他成员的血液样本进行分析,确定出一种名为hDEC2的变异基因。hDEC2是一种转录因子,会抑制某些基因的表达,并参与昼夜节律的调节。随后,科学家对小鼠和果蝇进行了基因改造。通过对转基因小鼠的脑电图(EEG)和肌电图(EMG)监测,他们发现,转基因小鼠的睡眠时间明显减少;在被强行剥夺了6个小时的睡眠后,转基因小鼠需要弥补的睡眠量也远比正常小鼠要少。

hDEC2的发现有助于揭开睡眠调整机制之谜。虽然hDEC2基因变异可能十分罕见,但它确实提供了一个探索睡眠调整机制的机会。了解了这些机制,科学家就可以通过某些干预手段来缓解患有睡眠障碍相关疾病患者的痛苦。这无疑将对未来人们的身心健康产生重大影响。

(据科学网)